IN THE CLAIMS:

Please substitute the following claims for the pending claims with the same number:

12. (currently amended) A method for limiting the operational life of software in a network environment, the method comprising:

providing a program applet with a password embedded therewithin to a client computer via a network, the password having a limited operational life;

receiving from said program applet via said network a request for information stored in a restricted access storage area of a server computer;

automatically receiving from said program applet said embedded password without manual entry of the password by a user, for authentication, whenever said receiving occurs;

authenticating said embedded password by the server computer and not by the program applet, whenever said receiving occurs;

thereafter providing said information to said program applet via said network while said embedded password is valid; and

invalidating said embedded password coincident with an invalidation event.

13. (previously presented) A method according to claim 12 wherein said invalidating comprises invalidating said embedded password at a predetermined time.

14. (previously presented) A method according to claim 12 wherein said invalidating comprises invalidating said embedded password after lapse of a predetermined time from when said request was received.

15. (previously presented) A method according to claim 12 wherein said invalidating comprises invalidating said embedded password upon the detection of a loss of communication with said client.

16. (canceled)

17. (canceled)

18. (previously presented) A method according to claim 12 wherein said providing comprises generating said embedded password.

27. (currently amended) A network-based software authentication system comprising a server computer, the server computer comprising:

a password generator;

password validation apparatus;

a restricted-access storage area;

a program applet; and

invalidation apparatus;

wherein said server is operative to:

a) cause said password generator to generate a password, the password having a limited operational life;

b) embed said password within said program applet, and provide said program applet with said password embedded therewithin to a client via a network;

c) receive a request for information and, whenever information requested is stored in the restricted-access storage area, automatically receive said embedded password, from said program applet via said network, for authentication, without manual entry of the password by a user;

d) authenticate said embedded password using said password validation apparatus and not by said program applet, whenever information requested is stored in the restricted-access storage area;

e) provide said information to said program applet via said network while said embedded password is valid; and

f) invalidate said embedded password using said invalidation apparatus coincident with an invalidation event.

28. (original) A system according to claim 27 wherein said invalidation event comprises the arrival of a predetermined time.

29. (previously presented) A system according to claim 27 wherein said invalidation event comprises the lapsing of a predetermined time from when said request was received.

30. (original) A system according to claim 27 wherein said invalidation event comprises the detection of a loss of communication with said client.

31. (canceled)

32. (canceled)

33. (previously presented) A system according to claim 27 wherein said password is generated at said server computer.